VPNを用いた学内ネットワークへの接続

服部 裕之
情報システム管理課

概 要

本学では、学外から学内向けサーバへのアクセスの為に、ダイヤルアップ接続用の受け口を学内の教職員・学生向けに用意している。ところが家庭からの常時接続や無線 LAN によるホットスポットなど、インターネットへの接続形態が多様化している昨今では、これらに対応した学内ネットワークへの接続手段を考慮する必要がある。

そこで、2002 年 7 月より、学内ネットワークへの新たな接続手段として、VPN (*Virtual Private Network*) による接続サービスを実験的に開始した [1] [2]。

本稿では VPN 接続実験サービス開始に先立って行った予備実験と、VPN 接続実験サービスの現状について報告する。

1 VPNとは

1.1 背景

VPN(Virtual Private Network) とは、インターネット上の任意の 2 地点間であたかもインターネット回線を専用回線であるかのように利用するネットワーク技術である。

VPN は、遠隔地の拠点間を専用回線ではなくインターネット回線を用いて相互に接続し、安価に企業内ネットワークを構築する場合や、営業職など社外にいることが多い社員に対して、自社ネットワークへの安全かつ安価なアクセス手段を提供する為によく利用されている。

本学の場合、VPN を活用すると、つぎのようなユーザからの要望に答えることが可能になる （図 1)。

1. 自宅と大学間が離れているため、大学へ直接 PPP 接続をするのは電話料金がかさむ。普段は、近所のインターネットプロバイダのアクセスポイントへ接続しているので、そのプロバイダ経由で大学のイントラネット、学内ネットワークのみアクセスが許可されている Web ページにアクセスしたい。

2. 自宅では、ADSL や ケーブルテレビのインターネット接続サービスなどを利用し、すでにインターネットとは常時接続している。それにもかかわらず、学内ネットワークのみアクセスが許可されている大学の Web ページにアクセスする時のみ、ネットワーク接続の方法をダイヤルアップ接続に変更するのは面倒である。設定をさほど変更せずに、大学のイントラネットにアクセスしたい。

3. 普段は大学へダイヤルアップ接続しているが、たまたま出張先から自分のコンピュータにアクセスする必要がでてきた。しかし、遠距離のため大学へ直接 PPP 接続をするのは、電話料金がかさむ。自分の契約しているインターネットプロバイダのアクセスポイントが出張先の近くにあるので、そこを利用して大学へ接続したい。

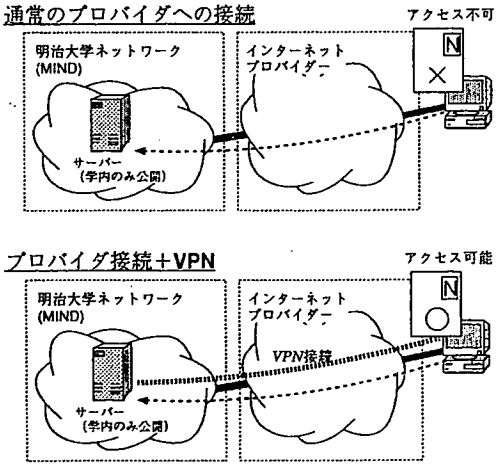


図 1 : VPN の概要

1.2 VPNを構成する技術

VPNは、「トンネリング」技術と「暗号」技術を組み合わせたものである。

「トンネリング」技術とは、ある特定の地点間でパケットをカプセル化して送信する技術のことである。この技術を用いると、IPプロトコルの転送のみ可能なネットワーク上でもIPXやAppleTalk、SNAなど別のプロトコルを転送することができる。

VPNで用いられるトンネリング方式には、主に次のものがある。

- L2F - *Layer 2 Forwarding*
  Cisco Systemsが開発したプロトコル。現在は、L2TPに統合。RFC 2341。
- PPTP - *Point to Point Tunneling Protocol*
  Microsoft, Lucent Technology, 3Comなどが開発したプロトコル。RFC 2637。
- L2TP - *Layer 2 Tunneling Protocol*
  L2FとPPTPを統合したプロトコル。RFC 2661。

ところで「トンネリング」技術を用いて、特定の2地点間での通信が可能になったとしても、第三者によってそのパケットの中身を解読されては、セキュリティ上、専用回線の代替として利用することはできない。そこでパケットの暗号化が必要となる。

VPNで用いられる暗号方式は、以下の通りである。

- MPPE - *Microsoft Point-To-Point Encryption Protocol*
  MicrosoftがPPTPの拡張として実装。
  40,56,128bitのRC4暗号方式を使用。
  RFC 3078。
- IPsec - *IP Security Protocol*
  ネットワーク層のセキュリティプロトコルとして規定。

VPNを行うためには、パケットのトンネリングおよび暗号処理を行う装置が必要である。インターネットを用いた企業内ネットワークの構築には、拠点毎にこのような装置が必要となる。

図2にパケットのトンネリングと暗号処理の概略を記載する。

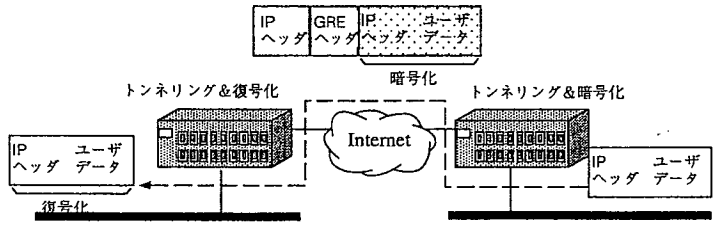


図2： トンネリングと暗号処理 (PPTP+MPPEの例)

2 VPN接続実験

VPN接続実験サービスを開始するにあたり、事前に機器の設定や動作確認の為の予備実験を行った。

予備実験は、以下の2通りの接続形態で行った。

実験1. ダイヤルアップ接続
PCをプロバイダにダイヤルアップ接続した上で、大学のVPNルータに対してVPN接続を試みる。

実験2. SOHOルータを用いた接続
家庭内にLAN環境を構築していることを想定する。
NAT機能を有効にしたSOHOルータをインターネットプロバイダにダイヤルアップ接続し、PCはSOHOルータを介してインターネットへLAN接続する。その状態で、PCから大学のVPNルータに対してVPN接続を試みる。

2.1 システム構成

本実験におけるシステム構成を図3に示す。

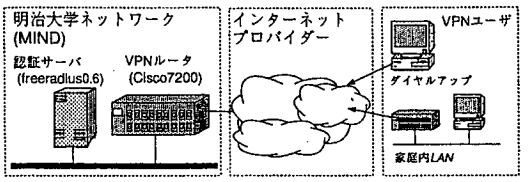


図3： システム構成

VPN ルータおよび認証サーバの構成は次の通りである。

VPN ルータ

機種	Cisco7206
ホスト名	vpn.mind.meiji.ac.jp
IOS バージョン	12.1(11b)E1
ハードウェア暗号モジュール	あり

認証サーバ

機種	富士通 Primepower1
OS バージョン	Solaris8
認証デーモン	Freeradius 0.6[3]

これらの機器を用いて、以下の VPN 接続に対応できるよう設定を行った。

認証プロトコル	PAP, MS-CHAP
トンネリング方式	PPTP
暗号方式	MPPE (40bit)

2.2 予備実験 1: ダイヤルアップ接続

2.2.1 概要

PC をインターネット・プロバイダにダイヤルアップ接続し、さらに大学の VPN ルータに VPN 接続を行う（図4）。

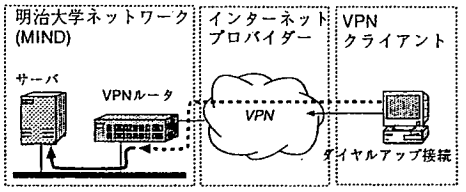


図4： ダイヤルアップ＋ VPN 接続

2.2.2 使用機材およびネットワーク環境

VPN クライアント側の PC の構成は次の通り。

ハードウェア	富士通 FMV-BIBLO LOOX S8/70
OS	Windows XP
ネットワーク	I/O データ USB-H64
	Kyocera PHS PC-C1

また、ダイヤルアップ接続先に指定したプロバイダに関する情報は次の通りである。

プロバイダ	OCN (NTT コミュニケーション)
アクセスポイント	東京
接続プロトコル	PIAFS2.1 (64Kbps)
IP アドレス	グローバル IP アドレス
	(例：61.119.232.159)

接続確認の為に用いた学内ネットワーク上のサーバは以下の通りで、いずれも通常はインターネットからアクセスすることはできない。学内のみに公開しているサーバである。

サーバ 1

機種	富士通 GP400S model10
ホスト名	tama-zoo.mind.meiji.ac.jp

サーバ 2

機種	富士通 SunFire280
ホスト名	mjuserv.mind.meiji.ac.jp

なお、VPN ルータ側の構成は、2.1 で述べた通りである。

2.2.3 動作確認

1. **VPN の確立と確認**
   PC～VPN ルータ間で VPN が確立したことを確認する。
   VPN の方式は、PPTP によるトンネリングおよび MPPE(40bit) による暗号化で、ユーザ認証は MS-CHAP で行う。
   VPN 接続の確認は、GUI および ipconfig コマンドを用いる。

2. **パケット到達確認**
   PC から大学内ネットワーク上のサーバにパケットが到達することを確認する。
   確認は、ping および traceroute コマンドを用いる。

3. **アプリケーションの動作確認**
   PC からネットワーク・アプリケーションを起動し、大学内ネットワーク上のサーバにアクセスする。
   確認は、telnet および Web ブラウザを用いる。

[動作確認 1] VPN の確立と確認

(VPN 接続後、PC のネットワーク状態を調査)

```
C:\> ipconfig /all

PPP adapter OCN(PIAFS 2.1):
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . . . . . : 00-53-45-00-00-00
Dhcp Enabled. . . . . . . . . . . : No
IP Address. . . . . . . . . . . . : 61.119.232.159
Subnet Mask . . . . . . . . . . . : 255.255.255.255
Default Gateway . . . . . . . . . : 61.119.232.159
DNS Servers . . . . . . . . . . . : 211.129.14.134
                                   211.129.12.43
PPP adapter 明治大学 SOHO VPN:
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . . . . . : 00-53-45-00-00-00
Dhcp Enabled. . . . . . . . . . . : No
IP Address. . . . . . . . . . . . : 133.26.20.21
Subnet Mask . . . . . . . . . . . : 255.255.255.255
Default Gateway . . . . . . . . . : 133.26.20.21
DNS Servers . . . . . . . . . . . : 133.26.136.30
```

(プロバイダから 61.119.232.159 が、VPN ルータから 133.26.20.21 が割当られている事を確認)

[動作確認 2] パケット到達確認

(VPN 接続後、PC から VPN ルータに対して ping を実行)

```
C:\> ping vpn.mind.meiji.ac.jp
Pinging vpn.mind.meiji.ac.jp [133.26.136.250] with 32 bytes of data:
Reply from 133.26.136.250: bytes=32 time=174ms TTL=243
Reply from 133.26.136.250: bytes=32 time=160ms TTL=243
        :
Ping statistics for 133.26.136.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 160ms, Maximum = 180ms, Average = 168ms
```

(VPN ルータまでの経路を調査)

```
C:\> tracert vpn.mind.meiji.ac.jp
Tracing route to vpn.mind.meiji.ac.jp [133.26.136.250]
  1   161 ms   157 ms   158 ms  61.112.57.6
  2   160 ms   157 ms   157 ms  61.112.57.1
  3   159 ms   158 ms   159 ms  211.16.14.201
  4   159 ms   156 ms   158 ms  211.6.5.67
  5   158 ms   158 ms   157 ms  210.254.187.117
  6   178 ms   156 ms   156 ms  61.207.0.34
  7   159 ms   157 ms   177 ms  210.173.176.27
  8   159 ms   155 ms   155 ms  nii-S1-P0-0.sinet.ad.jp [150.99.197.141]
  9   153 ms   176 ms   155 ms  JT-tokyo-S1-P8-0.sinet.ad.jp [150.99.197.21]
 10   159 ms   159 ms   158 ms  tokyo-S1-P9-0.sinet.ad.jp [150.99.197.38]
 11   159 ms   159 ms   157 ms  tokyo-11-P.sinet.ad.jp [150.99.197.226]
 12   160 ms   177 ms   174 ms  meiji-u.gw.sinet.ad.jp [150.99.170.24]
 13   177 ms   179 ms   177 ms  vpn.mind.meiji.ac.jp [133.26.136.250]
```

(PC から学内ホスト (tama-zoo) までの VPN 上の経路を調査)

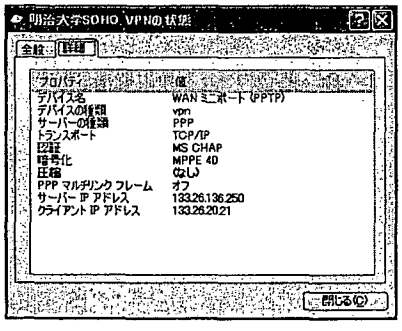
```
C:\> tracert tama-zoo.mind.meiji.ac.jp
Tracing route to tama-zoo.mind.meiji.ac.jp [133.26.208.73]
  1   232 ms   197 ms   238 ms  vpn.mind.meiji.ac.jp [133.26.136.250]
  2   190 ms   203 ms   177 ms  iku-gate-er.mind.meiji.ac.jp [133.26.136.254]
  3   209 ms   208 ms   198 ms  ocha-gate-er1.mind.meiji.ac.jp [192.168.3.1]
  4   198 ms   198 ms   247 ms  ct-e-4-224-s1.mind.meiji.ac.jp [133.26.225.246]
  5   419 ms   238 ms   175 ms  tama-zoo.mind.meiji.ac.jp [133.26.208.73]
```

[動作確認 3] アプリケーションの動作確認

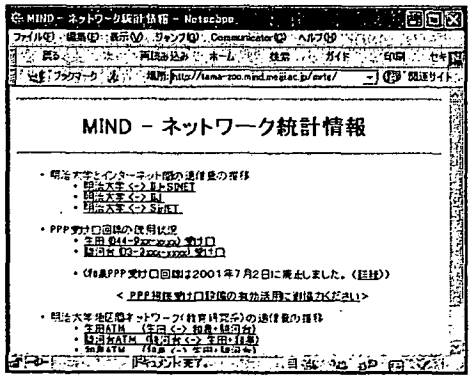
```
(学内ホスト (tama-zoo) に対し VPN 経由で telnet 接続)
  C:\> telnet  tama-zoo.mind.meiji.ac.jp

  SunOS 5.8

  login:

(学内ホスト (mjuserv) に対し VPN 経由で ftp 接続)
  C:\> ftp mjuserv.mind.meiji.ac.jp
  Connected to mjuserv.mind.meiji.ac.jp.
  220 mjuserv FTP server (Version wu-2.6.2(1) Mon Dec 3 15:15:16 JST 2001) ready.
  User (mjuserv.mind.meiji.ac.jp:(none)): ftp
  331 Guest login ok, send your complete e-mail address as password.
  Password:
  230-Welcome to Meiji Univ. anonymous ftp server.
  230- host='vpn-mobile21-20.mind.meiji.ac.jp'
  230-
  ftp>
```

「ネットワークの状態」を調べる。

PPTP+MPPE (40bit) を用いた VPN が確立していることを確認。



インターネットからはアクセスできない Web サーバ (http://tama-zoo.mind.meiji.ac.jp/) に対し、VPN 経由でアクセスができることを確認。



2.3 予備実験 2: SOHO ルータを用いた接続

2.3.1 概要

NAT 機能を有効にした SOHO ルータをプロバイダにダイヤルアップ接続し、PC は SOHO ルータを介してインターネットへ LAN 接続する。この状態で PC から大学の VPN ルータに対して VPN 接続する（図 5）。

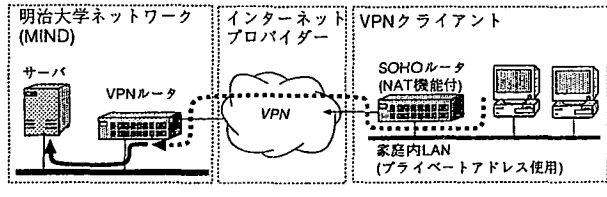


図 5 ： SOHO ルータ＋ VPN 接続

2.3.2 使用機材およびネットワーク環境

実験に使用した SOHO ルータの構成は次の通りである。

SOHO ルータ	NTT-ME MN128 SL11
NAT 機能	ON
IP マスカレード機能	ON
ローカル側 IP アドレス	192.168.0.1 (プライベートアドレス)

なお接続先のプロバイダおよび VPN クライアントの条件は、2.2 と同様である。

2.3.3 動作確認

動作確認の項目は 2.2.3 と同様である。

[動作確認 1] VPN の確立と確認

(VPN 接続後、PC のネットワーク状態を調査)

```
C:\> ipconfig /all
Ethernet adapter ローカル エリア接続
Connection-specific DNS Suffix  . : mind.meiji.ac.jp
Description . . . . . : Realtek RTL8139 Family PCI Fast Ethernet NIC
Physical Address. . . . . : 00-E0-00-59-FC-F0
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.0.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DNS Servers . . . . . : 192.168.0.1
PPP adapter 明治大学 SOHO VPN:
Connection-specific DNS Suffix  . :
Description . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . : 00-53-45-00-00-00
Dhcp Enabled. . . . . : No
IP Address. . . . . : 133.26.20.21
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 133.26.20.21
DNS Servers . . . . . : 133.26.136.30
                        133.26.192.3
```

(SOHO ルータから DHCP を用いて 192.168.0.3 が、VPN ルータから 133.26.20.21 が割当られている事を確認)

[動作確認 2] パケット到達確認

(VPN 接続後、PC から VPN ルータまでの経路を調査)

```
C:\> tracert vpn.mind.meiji.ac.jp
Tracing route to vpn.mind.meiji.ac.jp [133.26.136.250]
  1     4 ms     4 ms     4 ms  MN128-SOHO-PAL [192.168.0.1]
  2    44 ms    43 ms    43 ms  211.129.38.94
  3    46 ms    44 ms    46 ms  211.129.38.89
  4    46 ms    48 ms    47 ms  211.16.14.77
  5    46 ms    46 ms    46 ms  211.6.5.2
  6    46 ms    47 ms    46 ms  210.254.187.53
  7    44 ms    47 ms    47 ms  61.207.0.2
  8    48 ms    47 ms    46 ms  210.173.176.27
  9    46 ms    47 ms    45 ms  nii-S1-P0-0.sinet.ad.jp [150.99.197.141]
 10    45 ms    46 ms    46 ms  JT-tokyo-S1-P8-0.sinet.ad.jp [150.99.197.21]
 11    47 ms    48 ms    46 ms  tokyo-S1-P9-0.sinet.ad.jp [150.99.197.38]
 12    47 ms    47 ms    47 ms  tokyo-11-P.sinet.ad.jp [150.99.197.226]
 13    49 ms    50 ms    47 ms  meiji-u.gw.sinet.ad.jp [150.99.170.24]
 14    61 ms    61 ms    62 ms  vpn.mind.meiji.ac.jp [133.26.136.250]
```

(PC から学内ホスト (tama-zoo) までの VPN 上の経路を調査)

```
C:\> tracert tama-zoo.mind.meiji.ac.jp
Tracing route to tama-zoo.mind.meiji.ac.jp [133.26.208.73]
  1    74 ms    89 ms    70 ms  vpn.mind.meiji.ac.jp [133.26.136.250]
  2    70 ms    71 ms    75 ms  iku-gate-er.mind.meiji.ac.jp [133.26.136.254]
  3    82 ms    76 ms    76 ms  ocha-gate-er1.mind.meiji.ac.jp [192.168.3.1]
  4    73 ms    78 ms   111 ms  ct-e-4-224-s1.mind.meiji.ac.jp [133.26.225.246]
  5    93 ms   123 ms   111 ms  tama-zoo.mind.meiji.ac.jp [133.26.208.73]
```

2.4 VPN 接続実験サービス

以上の結果をふまえ、7月10日より「VPN 接続実験サービス」を開始した。

「VPN 接続実験サービス」は MIND 利用者であれば誰でも参加できるが、他の MIND の諸サービスと異なり「実験的なサービス」という位置付けである為、(1) 実験参加者はその正否にかかわらず実験レポートを提出する (2) 実験参加者はサポートを望まずに自力解決を原則とする、という特徴がある。これは、VPN 接続の正否は VPN クライアント側の環境に大きく依存しており、実験参加者にはトラブルを解決する為の一定以上のスキルが求められるためである。また、将来 VPN 接続を正式サービスとして展開する場合、サポートを行う為にはノウハウの共有と蓄積が必須である思われるからである。

8月1日現在、VPN 接続実験に参加している方は 26 名であり、レポートも徐々に集まりつつある。提出されたレポートは、Web で誰でもが閲覧可能である [4]。

3 まとめ

これまでの予備実験や VPN 接続実験参加者からの報告により、VPN 接続に関して幾つか注意すべき点が明かになった。

1. NAT ルータとの相性

   PPTP は、トンネリングを確立する為に、拡張 GRE(Generic Routing Encapsulation) ヘッダを用いている。GRE は汎用的なトンネリングプロトコルなのであるが、NAT 機能を有効にした SOHO ルータの中に、GRE に対応していないものが存在する。SOHO ルータのファームウェアのアップデートで対応している場合もあるが、注意が必要であろう。

2. VPN 接続の同時確立に関する制限

   SOHO ルータを用いた場合、ローカル側の複数の PC から同時に PPTP による VPN 接続を行うことはできない。これは、PPTP はエンドポイント間でのトンネルが1本に限定される為である。

3. Autoproxy 機能との相性

   Web ブラウザを利用の際、プロキシーサーバの設定でよく用いられるのが Autoproxy 機能である。これは、Javascript で記述された Autoproxy 用のファイルを Web ブラウザの起動時に読み込ませることによって、そのブラウザが使用する Proxy サーバのホスト名やポート番号を自動的に最適なものに設定するという機能である。

   Autoproxy ファイルの記述には、まず PC 自身の IP アドレスを調べ、それを元に最適な Proxy サーバを設定する場合が多いのであるが、VPN 接続を行うと、PC 自身の IP アドレスを VPN 接続確立後の IP アドレスではなく、プロバイダのアドレスを元に評価してしまうことが判った。

   この為に、VPN 接続後もインターネットに直接接続しているものとみなされ、Proxy サーバを経由したアクセスとならず、結果として VPN 接続後は、明治大学学外の Web サーバに接続できないという現象が発生した。

以上のように VPN 接続を行う際にはいくつかの留意すべき点があることが判った。

今後は、VPN ルータに対する負荷の計測や、認証サーバの安定性、L2TP の評価、セキュリティ上の強度などをさらに検討し、学内ネットワークへの正式な接続手段として利用者に提供できるようにする予定である。

参考文献

[1] "VPN 接続の実験サービス開始について", http://www.meiji.ac.jp/mind/mind-use/020604/0205-VPN.txt

[2] "VPN 接続実験サービス", http://www.meiji.ac.jp/mind/vpn/index.html

[3] "Freeradius", http://www.freeradius.org/

[4] "VPN 接続実験レポート・アーカイブ", http://shimauma.mind.meiji.ac.jp/vpn-report/